



Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS Policy for the Information Security Program

May 2005

TABLE OF CONTENTS

1. PURPOSE.....	1
2. BACKGROUND	1
3. SCOPE	5
4. POLICY	5
4.1. INFORMATION SECURITY MANAGEMENT CONTROLS	5
4.1.1. RISK ASSESSMENT (RA)	5
4.1.1.1. RISK ASSESSMENT POLICY AND PROCEDURES	5
4.1.1.2. SECURITY CATEGORIZATION	5
4.1.1.3. RISK ASSESSMENT	5
4.1.1.4. RISK ASSESSMENT UPDATE.....	6
4.1.1.5. VULNERABILITY SCANNING	6
4.1.2. PLANNING (PL)	6
4.1.2.1. SECURITY PLANNING POLICY AND PROCEDURES	6
4.1.2.2. SYSTEM SECURITY PLAN (SSP).....	6
4.1.2.3. SYSTEM SECURITY PLAN UPDATE	6
4.1.2.4. RULES OF BEHAVIOR (ROB).....	7
4.1.2.5. PRIVACY IMPACT ASSESSMENT (PIA).....	7
4.1.3. SYSTEM AND SERVICES ACQUISITION (SA)	8
4.1.3.1. SYSTEM & SERVICES ACQUISITION POLICY AND PROCEDURES	8
4.1.3.2. ALLOCATION OF RESOURCES	8
4.1.3.3. LIFE CYCLE SUPPORT	8
4.1.3.4. ACQUISITIONS	8
4.1.3.5. INFORMATION SYSTEM DOCUMENTATION	9
4.1.3.6. SOFTWARE USAGE RESTRICTIONS	9
4.1.3.7. USER INSTALLED SOFTWARE	9
4.1.3.8. SECURITY DESIGN PRINCIPLES	9
4.1.3.9. OUTSOURCED INFORMATION SYSTEM SERVICES	9
4.1.3.10. DEVELOPER CONFIGURATION MANAGEMENT (CM)	10
4.1.3.11. DEVELOPER SECURITY TESTING	10
4.1.4. CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS (CA).....	10
4.1.4.1. CERTIFICATION, ACCREDITATION, & SECURITY ASSESSMENTS POLICIES AND PROCEDURES	10
4.1.4.2. SECURITY ASSESSMENTS.....	11
4.1.4.3. INFORMATION SYSTEM CONNECTIONS	11
4.1.4.4. SECURITY CERTIFICATION	11
4.1.4.5. PLAN OF ACTION & MILESTONES (POA&M)	11
4.1.4.6. SECURITY ACCREDITATION	11
4.1.4.7. CONTINUOUS MONITORING	12
4.2. INFORMATION SECURITY OPERATIONAL CONTROLS	12

4.2.1.	PERSONNEL SECURITY (PS)	12
4.2.1.1.	PERSONNEL SECURITY POLICY AND PROCEDURES	12
4.2.1.2.	POSITION CATEGORIZATION	12
4.2.1.3.	PERSONNEL SCREENING	12
4.2.1.4.	PERSONNEL TERMINATION	12
4.2.1.5.	PERSONNEL TRANSFER	13
4.2.1.6.	ACCESS AGREEMENTS	13
4.2.1.7.	THIRD PARTY PERSONNEL SECURITY	13
4.2.1.8.	PERSONNEL SANCTIONS	13
4.2.2.	PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)	13
4.2.2.1.	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	13
4.2.2.2.	PHYSICAL ACCESS AUTHORIZATION	14
4.2.2.3.	PHYSICAL ACCESS CONTROL	14
4.2.2.4.	ACCESS CONTROL FOR TRANSMISSION MEDIUM	14
4.2.2.5.	ACCESS CONTROL FOR DISPLAY MEDIUM	14
4.2.2.6.	MONITORING PHYSICAL ACCESS	14
4.2.2.7.	VISITOR CONTROL	14
4.2.2.8.	ACCESS LOGS	15
4.2.2.9.	POWER EQUIPMENT & POWER CABLING	15
4.2.2.10.	EMERGENCY SHUTOFF	15
4.2.2.11.	EMERGENCY POWER	15
4.2.2.12.	EMERGENCY LIGHTING	15
4.2.2.13.	FIRE PROTECTION	15
4.2.2.14.	TEMPERATURE AND HUMIDITY CONTROLS	16
4.2.2.15.	WATER DAMAGE PROTECTION	16
4.2.2.16.	DELIVERY & REMOVAL	16
4.2.2.17.	ALTERNATE WORKSITE	16
4.2.3.	CONTINGENCY PLANNING (CP)	16
4.2.3.1.	CONTINGENCY PLANNING POLICY AND PROCEDURES	16
4.2.3.2.	CONTINGENCY PLAN	17
4.2.3.3.	CONTINGENCY TRAINING	17
4.2.3.4.	CONTINGENCY PLAN TESTING	17
4.2.3.5.	CONTINGENCY PLAN UPDATE	17
4.2.3.6.	ALTERNATE STORAGE SITES	17
4.2.3.7.	ALTERNATE PROCESSING SITES	17
4.2.3.8.	TELECOMMUNICATION SERVICES	18
4.2.3.9.	INFORMATION SYSTEM BACKUP	18
4.2.3.10.	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	18
4.2.4.	CONFIGURATION MANAGEMENT (CM)	18
4.2.4.1.	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	18
4.2.4.2.	BASELINE CONFIGURATION	19
4.2.4.3.	CONFIGURATION CHANGE CONTROL	19
4.2.4.4.	MONITORING CHANGE ACTIVITY	19
4.2.4.5.	ACCESS RESTRICTION FOR CHANGE	19
4.2.4.6.	CONFIGURATION SETTINGS	20

4.2.4.7.	LEAST FUNCTIONALITY	20
4.2.5.	MAINTENANCE	20
4.2.5.1.	SYSTEM MAINTENANCE POLICY AND PROCEDURES	20
4.2.5.2.	PERIODIC MAINTENANCE	20
4.2.5.3.	MAINTENANCE TOOLS.....	20
4.2.5.4.	REMOTE MAINTENANCE	21
4.2.5.5.	MAINTENANCE PERSONNEL.....	21
4.2.5.6.	TIMELY MAINTENANCE.....	21
4.2.6.	SYSTEM AND INFORMATION INTEGRITY (SI)	21
4.2.6.1.	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES ..	21
4.2.6.2.	FLAW REMEDIATION	21
4.2.6.3.	MALICIOUS CODE PROTECTION	21
4.2.6.4.	INTRUSION DETECTION TOOLS AND TECHNIQUES	22
4.2.6.5.	SECURITY ALERTS AND ADVISORIES	22
4.2.6.6.	SECURITY FUNCTIONALITY VERIFICATION	22
4.2.6.7.	SOFTWARE AND INFORMATION INTEGRITY	22
4.2.6.8.	SPAM AND SPYWARE PROTECTION	22
4.2.6.9.	INFORMATION INPUT RESTRICTIONS	22
4.2.6.10.	INFORMATION INPUT ACCURACY, COMPLETENESS, AND VALIDITY ...	23
4.2.6.11.	ERROR HANDLING.....	23
4.2.6.12.	INFORMATION OUTPUT HANDLING AND RETENTION	23
4.2.7.	MEDIA PROTECTION (MP)	23
4.2.7.1.	MEDIA PROTECTION POLICY AND PROCEDURES	23
4.2.7.2.	MEDIA ACCESS.....	23
4.2.7.3.	MEDIA LABELING	23
4.2.7.4.	MEDIA STORAGE	23
4.2.7.5.	MEDIA TRANSPORT.....	24
4.2.7.6.	MEDIA SANITIZATION	24
4.2.7.7.	MEDIA DESTRUCTION AND DISPOSAL	24
4.2.8.	INCIDENT RESPONSE (IR)	24
4.2.8.1.	INCIDENT RESPONSE POLICY AND PROCEDURES	24
4.2.8.2.	INCIDENT RESPONSE TRAINING	24
4.2.8.3.	INCIDENT RESPONSE TESTING	24
4.2.8.4.	INCIDENT HANDLING	25
4.2.8.5.	INCIDENT MONITORING	25
4.2.8.6.	INCIDENT REPORTING.....	25
4.2.8.7.	INCIDENT RESPONSE ASSISTANCE.....	25
4.2.9.	AWARENESS AND TRAINING (AT).....	25
4.2.9.1.	SECURITY AWARENESS & TRAINING POLICY AND PROCEDURES	25
4.2.9.2.	SECURITY AWARENESS	25
4.2.9.3.	SECURITY TRAINING	26
4.2.9.4.	SECURITY TRAINING RECORDS.....	26
4.3.	INFORMATION SECURITY TECHNICAL CONTROLS	26
4.3.1.	IDENTIFICATION AND AUTHENTICATION (IA)	26
4.3.1.1.	IDENTIFICATION & AUTHENTICATION POLICY AND PROCEDURES	26
4.3.1.2.	USER IDENTIFICATION AND AUTHENTICATION	26

4.3.1.3.	DEVICE AND HOST IDENTIFICATION & AUNTHENTICATION	26
4.3.1.4.	IDENTIFIER MANAGEMENT	26
4.3.1.5.	AUTHENTICATOR MANAGEMENT	27
4.3.1.6.	AUTHENTICATOR FEEDBACK	27
4.3.1.7.	CRYPTOGRAPHIC MODULE AUTHENTICATION	27
4.3.2.	ACCESS CONTROL (AC).....	27
4.3.2.1.	ACCESS CONTROL POLICY AND PROCEDURES	27
4.3.2.2.	ACCOUNT MANAGEMENT.....	28
4.3.2.3.	ACCESS ENFORCEMENT	28
4.3.2.4.	INFORMATION FLOW ENFORCEMENT	28
4.3.2.5.	SEPARATION OF DUTIES.....	28
4.3.2.6.	LEAST PRIVILEGE.....	28
4.3.2.7.	UNSUCCESSFUL LOG-ON ATTEMPTS	29
4.3.2.8.	SYSTEM USE NOTIFICATION	29
4.3.2.9.	PREVIOUS LOG-ON NOTIFICATION.....	29
4.3.2.10.	CURRENT SESSION CONTROL	29
4.3.2.11.	SESSION LOCK.....	29
4.3.2.12.	SESSION TERMINATION	29
4.3.2.13.	SUPERVISION AND REVIEW — ACCESS CONTROL.....	29
4.3.2.14.	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	30
4.3.2.15.	AUTOMATED MARKING.....	30
4.3.2.16.	AUTOMATED LABELING.....	30
4.3.2.17.	REMOTE ACCESS	30
4.3.2.18.	WIRELESS ACCESS RESTRICTION	30
4.3.2.19.	ACCESS CONTROL FOR PORTABLE AND MOBILE SYSTEMS.....	30
4.3.2.20.	PERSONALLY-OWNED INFORMATION SYSTEMS.....	31
4.3.3.	AUDIT AND ACCOUNTABILITY (AU)	31
4.3.3.1.	AUDIT & ACCOUNTABILITY POLICY AND PROCEDURES	31
4.3.3.2.	AUDITABLE EVENTS.....	31
4.3.3.3.	CONTENT OF AUDIT RECORDS	31
4.3.3.4.	AUDIT STORAGE CAPACITY	31
4.3.3.5.	AUDIT PROCESSING	32
4.3.3.6.	AUDIT MONITORING, ANALYSIS, AND REPORTING.....	32
4.3.3.7.	AUDIT REDUCTION AND REPORT GENERATION.....	32
4.3.3.8.	TIME STAMPS.....	32
4.3.3.9.	PROTECTION OF AUDIT INFORMATION.....	32
4.3.3.10.	NON-REPUDIATION	32
4.3.3.11.	AUDIT RETENTION	32
4.3.4.	SYSTEM AND COMMUNICATIONS PROTECTION (SC)	32
4.3.4.1.	SYSTEM & COMMUNICATIONS PROTECTION POLICY AND PROCEDURES.....	32
4.3.4.2.	APPLICATION PARTITIONING.....	33
4.3.4.3.	SECURITY FUNCTION ISOLATION	33
4.3.4.4.	INFORMATION REMNANTS	33
4.3.4.5.	DENIAL OF SERVICE PROTECTION	33

4.3.4.6.	RESOURCE PRIORITY	33
4.3.4.7.	BOUNDARY PROTECTION	33
4.3.4.8.	TRANSMISSION INTEGRITY	34
4.3.4.9.	TRANSMISSION CONFIDENTIALITY	34
4.3.4.10.	NETWORK DISCONNECT.....	34
4.3.4.11.	TRUSTED PATH.....	34
4.3.4.12.	CRYPTOGRAPHIC KEY MANAGEMENT.....	34
4.3.4.13.	USE OF VALIDATED CRYPTOGRAPHY	34
4.3.4.14.	PUBLIC ACCESS PROTECTIONS	34
4.3.4.15.	COLLABORATIVE COMPUTING.....	34
4.3.4.16.	TRANSMISSION OF SECURITY PARAMETERS	35
4.3.4.17.	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	35
4.3.4.18.	MOBILE CODE.....	35
4.3.4.19.	VOICE OVER INTERNET PROTOCOL	35
4.4.	INVESTMENT MANAGEMENT LEVEL AND PROJECT MANAGEMENT	
	LEVEL REVIEWS	35
5.	ROLES AND RESPONSIBILITIES.....	36
5.1.	CMS ADMINISTRATOR.....	36
5.2.	CMS CHIEF INFORMATION OFFICER (CIO).....	36
5.3.	DIRECTOR, SYSTEMS SECURITY GROUP (SSG).....	37
5.4.	SENIOR ISSO	37
5.5.	COMPONENT ISSO	37
5.6.	BUSINESS OWNERS/PARTNERS AND SYSTEMS OWNERS/MANAGERS	37
5.7.	SYSTEM ADMINISTRATOR	38
5.8.	SYSTEM MAINTAINER / DEVELOPER.....	38
5.9.	CMS EMPLOYEES.....	38
5.10.	USERS.....	38
6.	APPLICABLE LAWS/GUIDANCE	39
7.	EFFECTIVE DATES	39
8.	INFORMATION AND ASSISTANCE	39
9.	APPROVED	39
10.	ATTACHMENTS	39

1. PURPOSE

This document creates the Centers for Medicare & Medicaid Services (CMS) Information Security (IS) Program Policy. The IS Program Policy aims to reduce the risk, and minimize the effect of security incidents. By establishing the ground rules under which the CMS shall operate its information systems, the formation of the CMS IS Program Policy is driven by many factors, the key one being **Risk**.

All CMS employees, contractors, sub-contractors, and their respective facilities supporting CMS business missions shall observe the individual policy statements. Some policies are explicitly for persons with a specific job function, e.g. the System Administrator; otherwise, all personnel supporting CMS business functions shall comply with the policies.

2. BACKGROUND

As the Agency charged with administering the Medicare, Medicaid, and State Children's Health Insurance Programs, CMS collects, generates, and stores financial, health care, and other sensitive information. Most of this information relates to the health care provided to the nation's Medicare and Medicaid beneficiaries and has access restrictions required by legislative and regulatory directives. As the information's trusted custodian, CMS must protect and ensure the confidentiality, integrity, and availability (CIA) of all its information regardless of how it is created, distributed, or stored.

To safeguard the CIA of its information and information systems effectively, CMS has established an enterprise-wide IS Program. As part of this program, security controls must be implemented to protect all information assets, including hardware, systems, software, and data. These controls must be designed to ensure compliance with all federal legislation, policies and standards (e.g. by managing risk; facilitating change control; reporting and responding to security incidents, intrusions, or violations; and formulating contracts).

The CMS IS Program Policies address the reduction in risks to information resources through adoption of preventive measures and controls designed to detect any errors that occur. It also addresses the recovery of information resources in the event of a disaster. For ease of use, the CMS IS Program Policy is organized into **classes and categories**. CMS has established three classes of IS controls - management, operational, and technical. This structure is consistent with the guidance established by the National Institute of Standards and Technology (NIST).

Management controls involve those safeguards and countermeasures that manage the security of the information and information systems and the associated risk to the Agency's assets and operations. There are **four** categories of policy within the management class that address:

- (i). Risk Assessment (RA);
- (ii). Security Planning;
- (iii). Systems and Services Acquisition; and
- (iv). Certification, Accreditation, and Security Assessments.

Operational controls support the day-to-day procedures and mechanisms to protect CMS' information and information systems. There are **nine** categories of policy within the operational class that address:

- (i). Personnel Security;
- (ii). Physical and Environmental Protection;
- (iii). Contingency Planning;

- (iv). Configuration Management;
- (v). Maintenance;
- (vi). System and Information Integrity;
- (vii). Media Protection;
- (viii). Incident Response; and
- (ix). Awareness and Training.

Technical controls are those security mechanisms employed within an information system's hardware, software, or firmware to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction. They are used to authorize or restrict the activities of all levels of users within an individual system by employing access based on a least-privileged and need-to-know approach. There are **four** categories of policy within the technical class that address:

- (i). Identification and Authentication;
- (ii). Access Control;
- (iii). Audit and Accountability; and
- (iv). System and Communications Protection.

IS PROGRAM ACTIVITIES

This section describes some of the key activities in an organizational IS program. These activities are conducted within the system developmental life-cycle.

Security Categorization

Security categorization establishes three impact levels (low, moderate, high) for each of the stated security objectives, i.e., CIA, relevant to securing information resource.

Risk Assessment

In accordance with the provisions of Federal Information System Management Act (FISMA), IS programs are required to conduct a periodic assessment of risks, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization.

Security Planning

In accordance with the provisions of FISMA, IS Programs are required to have plans for providing adequate IS for networks, facilities, information systems, or groups of information systems, as appropriate.

Security Control Development

The security controls, which are described in the security plans, shall be designed, developed, and implemented. For information systems in operation, the development or integration of additional security controls or the modification of selected controls may be necessary.

Developmental Security Test and Evaluation (ST&E)

The security controls must be tested and evaluated prior to deployment to ensure that the controls are effective. An ST&E plan is developed to test the security controls. This plan guides the developmental security testing and evaluation of the security controls and provides feedback to information system owners, developers, and integrators.

Security Control Integration

The integration of security controls occurs at the operational sites where the information systems are to be deployed for operations.

Security Control Verification

In accordance with the provisions of FISMA, periodic testing and evaluation of the security controls in an information system are required in order to ensure that the controls are implemented effectively. The comprehensive evaluation of security control effectiveness through established verification techniques and procedures, also known as security certification, is a critical activity conducted by the organization or by an independent third party on behalf of the organization.

Security Authorization

In accordance with the provisions of Office of Management and Budget (OMB) Circular A-130, a security authorization of an information system to process, store, or transmit information is required. This authorization, i.e., security accreditation granted by a senior organizational official, is based on the verified effectiveness of security controls to some agreed-upon-level of assurance together with an identified risk to the organization's operation or assets.

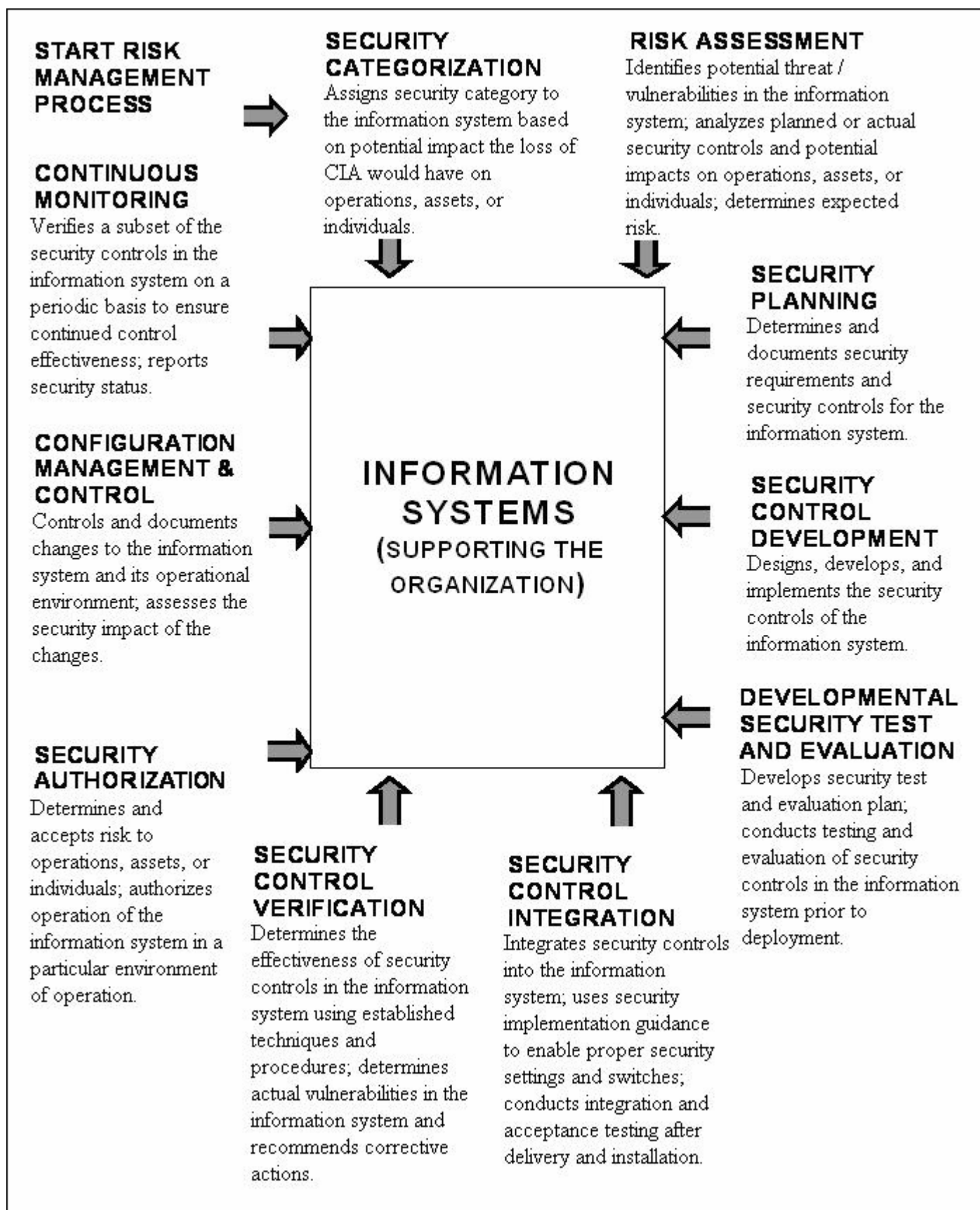
Configuration and Management Control

Changes to an information system can have a significant impact on the security of the system. Configuration management procedures are critical to the establishment of an initial baseline of hardware, software, and firmware components for an information system and the subsequent control and maintenance of an accurate inventory of changes to the system.

On-going Monitoring

In accordance with the provisions of FISMA, periodic testing and evaluation of security controls in an information system are required on an on-going basis to ensure that the controls continue to be effective in their application. The on-going monitoring of security control effectiveness can be accomplished in a variety of ways including security reviews, self-assessments, security testing and evaluation, or audits.

The following figure illustrates key IS program activities and the impact of those activities on the organization's information systems. Note the existence of the categories within the management, operational and technical classes throughout the diagram.



3. SCOPE

This policy applies to all CMS employees, contractors, sub-contractors, and their respective facilities supporting CMS business missions, wherever CMS data is stored or processed. This policy applies to all CMS information, information systems, IT activities and IT assets owned, leased, controlled or used by CMS, CMS' agents, contractors or other business partners.

4. POLICY

4.1. INFORMATION SECURITY MANAGEMENT CONTROLS

4.1.1. RISK ASSESSMENT (RA)

4.1.1.1. RISK ASSESSMENT POLICY AND PROCEDURES

All CMS applications and systems shall be covered by a Business RA and an IS RA. The RA shall be consistent with NIST Special Publication (SP) 800-30. Formal documented procedures shall be developed, disseminated, and reviewed/updated periodically to facilitate the implementation of the RA policy and associated risk assessment controls.

4.1.1.2. SECURITY CATEGORIZATION

CMS information systems and the information processed, stored, or transmitted by the system shall be categorized in accordance with Federal Information Processing Standards (FIPS) 199 and NIST SP 800-60. The security categorization (including supporting rationale) shall be explicitly documented. Designated senior-level official within CMS shall review and approve the security categorizations. CMS shall conduct security categorizations as an organization-wide activity with the involvement of the Chief Information Officer (CIO), senior agency IS officer, information system owners, and information owners.

4.1.1.3. RISK ASSESSMENT

An assessment of risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of CMS shall be performed. The RA shall be consistent with NIST SP 800-30. Based on the operation of the information system, the RA shall take into account vulnerabilities, threat sources, and security controls in place to determine the resulting level of residual risk posed to CMS operations, CMS assets, or individuals.

Any findings from authorized reviews of CMS systems shall be evaluated as to the impact of the vulnerability on the information system. Any identified weaknesses shall be documented by the system owner and addressed by mitigating the risk, accepting the risk with explanation or submitting Corrective Action Plan. These findings shall be subject to reporting requirements as established by federal law, OMB regulation or Departmental policy.

4.1.1.4. RISK ASSESSMENT UPDATE

The RA shall be performed and documented every three years and whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.1.4.6, Security Accreditation.

4.1.1.5. VULNERABILITY SCANNING

Appropriate vulnerability assessment tools and techniques shall be implemented by CMS. Selected personnel shall be trained in their use and maintenance. CMS shall conduct periodic testing of its security posture by scanning its information systems with vulnerability tools. The information obtained from the vulnerability scanning process shall be shared with appropriate personnel throughout the organization on a “need to know” basis to help eliminate similar vulnerabilities in other information systems. The activities of employees using CMS Internet and e-mail resources shall be subject to monitoring by system or security personnel without notice.

4.1.2. PLANNING (PL)

4.1.2.1. SECURITY PLANNING POLICY AND PROCEDURES

All CMS information systems shall be documented in a System Security Plan (SSP), which is compliant with OMB Circular A-130 and consistent with NIST SP 800-18. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is the basis for system accreditation, and subject to reporting requirements as established by federal law, OMB regulation or Departmental policy.

4.1.2.2. SYSTEM SECURITY PLAN (SSP)

All CMS information systems shall be covered by an SSP, which is compliant with OMB Circular A-130 and consistent with the intent of NIST SP 800-18. The SSP shall document the operation and security requirements of the system / application and the controls in place for meeting those requirements. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is subject to reporting requirements as established by federal law, OMB regulation or Departmental policy.

4.1.2.3. SYSTEM SECURITY PLAN UPDATE

The SSP shall be reviewed and updated to reflect current conditions every three (3) years or whenever there are significant changes made to the information system, facilities, or other conditions that may impact security; when the data sensitivity level increases; after a serious security violation; due to changes in the threat environment; or when the previous accreditation expires.

4.1.2.4. RULES OF BEHAVIOR (ROB)

ROBs shall be established, and made readily available, to delineate clearly user responsibilities and expected behavior of all system owners, users, operators and administrators. Before authorizing access to the information system CMS shall receive a signed acknowledgement from all users indicating that they have read, understand, and agree to abide by the rules of behavior. Specific rules of behavior shall be established to govern work-at-home users who access CMS information systems.

Limited personal use of Agency-owned or leased equipment and resources shall be considered to be a permitted use of Agency-owned or leased equipment and resources when the following conditions are met:

1. Such use involves minimal additional expense to the Agency;
2. Such use does not interfere with the mission or operation of the Agency;
3. Such use does not violate the Standards of Ethical Conduct for Employees of the Executive Branch;
4. Such use does not overburden any Agency information resources;
5. Such use is not otherwise prohibited under this policy; and
6. Any use of CMS Internet and e-mail resources shall be made with the understanding that such use is not secure, private or anonymous.

The following uses of Agency-owned or leased equipment or resources, either during working or non-working hours, are strictly prohibited:

1. Activities that are in violation of law, Government-wide rule or regulation or that are otherwise inappropriate for the workplace;
2. Activities that would compromise the security of any Government host computer. This includes, but is not limited to, sharing or disclosing log-on identification and passwords;
3. Fund-raising or partisan political activities, endorsements of any products or services or participation in any lobbying activity;
4. All e-mail communications to groups of employees that are subject to approval prior to distribution and have not been approved by the Agency (e.g., retirement announcements, Union notices or announcements, charitable solicitations); and
5. Employees shall not use the Internet for any purpose, which would reflect negatively on the Agency or its employees.

All employees shall have a reasonable expectation of privacy in the workplace. However, employee users of Agency-owned or leased equipment and resources shall not have an expectation of privacy while using such equipment or resources at any time, including times of permitted personal usage as set forth in this policy. To the extent that employees desire to protect their privacy, employees shall not use Agency-owned or leased equipment and resources.

4.1.2.5. PRIVACY IMPACT ASSESSMENT (PIA)

PIA's shall be conducted for CMS information systems, which are compliant with the E-Government Act of 2002, OMB Memorandum 03-22, and the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations.

4.1.3. SYSTEM AND SERVICES ACQUISITION (SA)

4.1.3.1. SYSTEM & SERVICES ACQUISITION POLICY AND PROCEDURES

Documented procedures shall be developed to facilitate the implementation of the system and services acquisition security controls in all system and services acquisitions. Procedures shall be consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.

4.1.3.2. ALLOCATION OF RESOURCES

As part of the capital planning and investment control processes, CMS shall determine, document, and allocate the resources required to protect CMS information systems adequately. IS requirements shall be included in mission / business case planning, and a separate line item shall be established in CMS' programming and budgeting documentation for the implementation and management of information systems security.

4.1.3.3. LIFE CYCLE SUPPORT

A uniform System Development Life-Cycle (SDLC) methodology shall be established and followed to manage all CMS information systems.

4.1.3.4. ACQUISITIONS

Based on an assessment of risk, security requirements and / or security specifications shall be included, either explicitly or by reference, in information system acquisition contracts.

Solicitation Documents

Solicitation documents (e.g. Request for Proposal) for any CMS information system shall include, either explicitly or by reference, security requirements that describe:

- (i). required security capabilities;
- (ii). required design and development processes;
- (iii). required test and evaluation procedures; and
- (iv). required documentation.

The requirements in the solicitation documents shall permit updating security controls as new threats / vulnerabilities are identified and as new technologies are implemented

Use of evaluated and validated products

For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology (IT) products, when multiple products meet CMS requirements, preference shall be given to products that have been evaluated and validated through one or more of the following sources:

1. The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme;
2. The International Common Criteria Recognition Arrangements; and
3. The NIST Cryptographic Module Validation Program.

Configuration Settings and Implementation Guidance

The information system required documentation shall include security configuration settings, including documentation explaining exceptions to the standard, and security implementation guidance.

4.1.3.5. INFORMATION SYSTEM DOCUMENTATION

Procedures shall be developed, documented, and implemented effectively to ensure that adequate documentation for all CMS information systems and its constituent components is available, protected when required, and distributed only to authorized personnel. The administrative and user guides and / or manuals shall include information on configuring, installing, and operating the information system, and for optimizing the system's security features. The guides and / or manuals shall be reviewed periodically, and, if necessary, updated as new vulnerabilities are identified and / or new security controls are added.

4.1.3.6. SOFTWARE USAGE RESTRICTIONS

All software or shareware and associated documentation used on CMS information systems shall be deployed and maintained in accordance with appropriate license agreements and copyright laws. Software associated documentation protected by quantity licenses shall be managed through a tracking system to control copying and distribution. All other uses not specifically authorized by the license agreement shall be prohibited. The use of publicly accessible peer-to-peer file sharing technology shall be controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

4.1.3.7. USER INSTALLED SOFTWARE

All users shall be restricted from downloading or installing software, unless explicitly authorized in writing by the CIO or his / her designated representative. Users that have been granted such authorization may download and install only CMS-approved software. The use of install-on-demand software shall be restricted.

4.1.3.8. SECURITY DESIGN PRINCIPLES

CMS information systems shall be designed and implemented using accepted security engineering principles.

4.1.3.9. OUTSOURCED INFORMATION SYSTEM SERVICES

All outsourced information system services shall include specific provisions requiring the service provider to comply with CMS IS policies, standards and guidelines and shall be monitored for compliance. CMS shall define the remedies for any loss, disruption or damage caused by the service provider's failure to comply. Service providers shall be prohibited from outsourcing any system function overseas, unless explicitly authorized, in writing, by the CIO, or his / her designated representatives.

4.1.3.10. DEVELOPER CONFIGURATION MANAGEMENT (CM)

Information system developers shall develop, document, and implement a configuration management plan for each information system under development. The configuration management plan shall address change control mechanisms during development, change authorization requirements, and security flaw identification, tracking, and remediation processes.

4.1.3.11. DEVELOPER SECURITY TESTING

Information system developers shall develop, document, and implement an ST&E plan for each information system under development. The developmental ST&E results shall be documented. The developmental security test results may be used in support of the security certification and accreditation (C&A) process for the information system.

4.1.4. CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS (CA)

4.1.4.1. CERTIFICATION, ACCREDITATION, & SECURITY ASSESSMENTS POLICIES AND PROCEDURES

All General Support Systems (GSSs) (i.e., hardware and related infrastructure) and Major Applications (MAs) (i.e., application code) shall be certified by the system owner and accredited by the CIO or his / her designated representative to ensure that the security controls for each GSS or MA mitigate risk to an acceptable level for protecting the CIA of CMS information and information systems.

Unless there are major changes to a system, re-certification and re-accreditation of GSSs MAs and application systems shall be performed every three (3) years. If there are major changes to the GSS, MA, or application system, re-certification and re-accreditation shall be performed whenever the changes occur. Also, re-accreditation and / or re-certification shall be performed upon the completion of the certification / accreditation action lists, in the case of an interim accreditation. Further, the requirements for re-accreditation / re-certification are listed in section 4.1.4.6, Security Accreditation.

If the CMS CIO or his / her designee is not satisfied that the system is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. Interim approval shall be granted only by the CMS CIO or his / her designated representative in lieu of a full denial to process. Interim approval to operate is not a waiver of the requirement for management approval to process. The information system shall meet all requirements and receive management approval to process by the interim approval expiration date. No extensions of interim accreditation shall be granted except by the CMS CIO or his / her designated representatives.

As part of the system C&A an independent evaluation based on the system security level may be performed and the results analyzed. Considering the evaluation results from the system testing, RAs, SSP, independent system tests and evaluations, the system owner / manager and the system maintainer shall certify that the system meets the security requirements to the extent necessary to protect CMS information adequately and meets an acceptable level of risk. Final accreditation shall be made by the CIO or the Designated Accrediting Authority (DAA).

4.1.4.2. SECURITY ASSESSMENTS

Routine assessments of all CMS information systems shall be conducted prior to initial operational capability and authorization to operate; prior to each re-authorization to operate; or when a significant change to the information system occurs. Routine assessments of all CMS information systems shall determine if security controls are implemented correctly, are effective in their application and comply with security-applicable laws, Executive Orders, directives, regulations, CMS policies, standards, and guidelines. Routine self-assessments shall be conducted annually, in accordance with NIST SP 800-26 or an acceptable alternative methodology, to monitor the effectiveness of security controls. Findings are subject to reporting requirements as established by federal law, OMB regulation or Departmental policy.

System PIAs shall be completed by system business owners on an annual basis including all applications in operation. Section 4.1.2.5 provides references for this requirement.

4.1.4.3. INFORMATION SYSTEM CONNECTIONS

Management shall authorize in writing all connections to other information systems outside of the accreditation boundary including systems owned and operated by another program, organization, or contractor in compliance with established CMS connection rules and approval processes. The system interconnections, which are connections between infrastructure components of a system or application, shall be monitored / controlled on an on-going basis.

4.1.4.4. SECURITY CERTIFICATION

System owners shall conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The security certification process shall be integrated into and span across the SDLC. In addition, the system owner shall review the certification documentation annually, update the documentation where necessary to reflect any changes to the system, and submit a copy of the updated information to the CIO or his / her designated representative.

4.1.4.5. PLAN OF ACTION & MILESTONES (POA&M)

CMS shall develop, implement and update a POA&M based on the findings from security control assessments, security impact analyses and continuous monitoring activities. The POA&M shall document the planned, implemented, and evaluated corrective actions to repair any deficiencies discovered during the security control assessment, and to reduce or eliminate any known vulnerability in the information system.

4.1.4.6. SECURITY ACCREDITATION

In compliance with NIST SP 800-37, explicit authorization to operate the information system shall be received from the CIO or his / her designated representative prior to the system being placed into operations. If the authorization is an interim approval to operate then the authorization shall be granted based on the designated security category of the information system. An explicit corrective action plan shall be developed, implemented effectively, and

monitored by the authorizing official. Re-authorization shall be obtained prior to continued operation when:

- Substantial changes are made to the system;
- Changes in requirements result in the need to process data of a higher sensitivity;
- Changes occur to authorizing legislation or federal requirements;
- After the occurrence of a serious security violation which raises questions about the validity of an earlier certification; and
- Expiration of a previous accreditation.

4.1.4.7. CONTINUOUS MONITORING

Security controls in CMS information systems shall be monitored on an on-going basis. Selection criteria for control monitoring shall be established and a subset of the security controls employed within information systems shall be selected for continuous monitoring purposes.

4.2. INFORMATION SECURITY OPERATIONAL CONTROLS

4.2.1. PERSONNEL SECURITY (PS)

4.2.1.1. PERSONNEL SECURITY POLICY AND PROCEDURES

CMS information systems shall employ personnel security controls consistent with federal law and the OPM policies, directives, regulations, standards and guidelines. Procedures shall be developed to guide the implementation of personnel security controls.

4.2.1.2. POSITION CATEGORIZATION

A criticality / sensitivity rating (e.g. non-sensitive, national security and public trust) shall be assigned to all positions within CMS. The criticality / sensitivity rating shall be consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance. Screening criteria shall be established based on the information system access given to the individuals filling those positions. All positions shall be reviewed periodically for criticality / sensitivity rating.

4.2.1.3. PERSONNEL SCREENING

Prior to being granted access, all employees and contractors who require access to CMS information and information systems shall be screened and reinvestigated periodically, consistent with the criticality/sensitivity rating of the position prior to being granted access. For prospective employees, references shall be contacted and background checks shall be performed. Security agreements shall be required for employees and contractor assigned to work with mission critical information.

4.2.1.4. PERSONNEL TERMINATION

Termination procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information systems is removed upon personnel termination. Termination procedures shall address:

- exit interviews;

- return of all organizational information system-related property (keys, identification cards, passes, etc.);
- notification to security management;
- revocation of all system access privileges;
- immediately escorting employees terminated for cause out of CMS facilities; and
- hard disk back up and sanitization before re-issuance.

4.2.1.5. PERSONNEL TRANSFER

Transfer procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information systems no longer required in the new assignment is terminated upon personnel transfer. Transfer procedures shall address:

- Re-issuing appropriate organizational information system-related property (keys, identification cards, building passes, etc.);
- notification to security management;
- closing obsolete accounts and establishing new accounts; and
- revocation of all system access privileges (if applicable).

4.2.1.6. ACCESS AGREEMENTS

Individuals who require access to CMS information and information systems shall be required to complete appropriate access agreements, including, but not limited to, non-disclosure agreements, acceptable use agreements, ROB, and conflict-of-interest agreements.

4.2.1.7. THIRD PARTY PERSONNEL SECURITY

Personnel security controls employed by CMS service providers and third parties shall be documented, agreed to, implemented, and monitored for compliance and shall include provisions for security clearances, background checks, required expertise, and confidentiality agreements. Personnel security controls employed by service providers and third parties shall be compliant with CMS IS policies and procedures and consistent with NIST SP 800-35.

4.2.1.8. PERSONNEL SANCTIONS

CMS shall enforce formal personnel sanctions process for personnel who fail to comply with established CMS IS policies and procedures. The employee sanction process shall be consistent with applicable federal laws, policies, directives, regulations, standards and guidelines.

4.2.2. PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

4.2.2.1. PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Physical and environmental protection procedures shall be developed and implemented to protect all CMS IT infrastructure and assets from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft whether accidental or intentional. These procedures shall meet all federal, state and local building codes and be consistent with General Services Administration policies, directives, regulations, and guidelines.

4.2.2.2. PHYSICAL ACCESS AUTHORIZATION

Access lists of personnel with authorized access to facilities containing CMS information systems (except for those areas within the facilities officially designated as publicly accessible) shall be documented on standard forms, maintained on file, approved by appropriate organizational officials, and reviewed periodically, and, if necessary, updated. Appropriate authorization credentials (e.g., badges, identification cards, smart cards) shall be issued to authorized personnel. Personnel who no longer require access shall be removed promptly from all access lists.

4.2.2.3. PHYSICAL ACCESS CONTROL

Physical access control devices (e.g., keys, locks, combinations, and card-readers) and / or guards shall be used to control entry to and exit from facilities containing CMS information systems, except for areas and / or facilities officially designated as publicly accessible. Individual access authorizations shall be verified before granting access to facilities containing CMS information systems. Physical access control devices (e.g., keys, locks, combinations, key cards) shall be secured and inventoried on a regular basis.

Combinations and keys shall be changed promptly when lost, compromised, or when individuals are transferred or terminated. Re-entry to facilities during emergency-related events shall be restricted to authorized individuals only. Access to workstations and associated peripheral computing devices shall be appropriately controlled when located in areas designated as publicly accessible.

4.2.2.4. ACCESS CONTROL FOR TRANSMISSION MEDIUM

Physical access controls shall be established and implemented to protect against eavesdropping, in-transit modification, disruption, and / or physical tampering of CMS information system transmission lines that carry unencrypted information.

4.2.2.5. ACCESS CONTROL FOR DISPLAY MEDIUM

Physical access controls shall be established and implemented to prevent unauthorized individuals from observing CMS sensitive information displayed on information system devices.

4.2.2.6. MONITORING PHYSICAL ACCESS

Physical access to information systems shall be monitored for physical security compliance and to detect and respond to incidents. Appropriate CMS officials shall periodically review physical access logs, investigate apparent security violations or suspicious physical access activities, and take appropriate remedial action.

4.2.2.7. VISITOR CONTROL

Visitor controls shall be developed, documented, and implemented effectively to control access to sensitive facilities and restricted / controlled areas containing CMS information systems and systems / media libraries. Visitors shall be authenticated prior to being granted access to

facilities or areas other than areas designated as publicly accessible. Government contractors and others with permanent authorization credentials are not considered visitors.

4.2.2.8. ACCESS LOGS

Visitor access to sensitive facilities and restricted / controlled areas that contain CMS information systems shall be logged. The visitor access log shall contain:

- (i). the name and organization of the person visiting;
- (ii). signature of the visitor;
- (iii). form of identification;
- (iv). date of access;
- (v). time of entry and departure;
- (vi). purpose of visit; and
- (vii). name and organization of person visited.

Appropriate CMS officials shall periodically review the access logs, including after closeout.

4.2.2.9. POWER EQUIPMENT & POWER CABLING

Power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain safe power for CMS information systems.

4.2.2.10. EMERGENCY SHUTOFF

Emergency shut-off controls shall be developed, documented, and implemented effectively to provide the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.

4.2.2.11. EMERGENCY POWER

Emergency power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to facilitate an orderly shutdown of the CMS information system in the event of a primary power source loss.

4.2.2.12. EMERGENCY LIGHTING

Mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enhance safety and availability. Automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes shall be provided.

4.2.2.13. FIRE PROTECTION

Fire protection mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to prevent, detect, and respond to fire. Fire suppression and detection devices / systems that can be activated in the event of a fire shall be

employed and maintained. Fire suppression and detection devices / systems shall include, but not be limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

4.2.2.14. TEMPERATURE AND HUMIDITY CONTROLS

Temperature and humidity control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain (within acceptable levels) and monitor the temperature and humidity of facilities containing CMS information systems.

4.2.2.15. WATER DAMAGE PROTECTION

Building plumbing shall not endanger the CMS information system facility or, at a minimum, the shut-off valves and their operating procedures shall exist and shall be known. Procedures shall be developed, documented, and implemented effectively to reduce the potential damage from plumbing leaks.

4.2.2.16. DELIVERY & REMOVAL

Procedures shall be developed, documented, and implemented effectively to control the flow of equipment into and out of the organization. Appropriate officials shall authorize the delivery or removal of CMS information system-related equipment.

To avoid unauthorized access, delivery and removal controls shall be implemented to isolate delivery areas from sensitive facilities and restricted / controlled areas containing CMS information systems and media libraries.

4.2.2.17. ALTERNATE WORKSITE

Procedures shall be developed, documented, and implemented effectively to control information system security at alternate work sites. A method of communication shall be provided to employees at alternate worksites to report security issues or suspected security incidents.

4.2.3. CONTINGENCY PLANNING (CP)

4.2.3.1. CONTINGENCY PLANNING POLICY AND PROCEDURES

All major CMS information systems shall be covered by a contingency plan that complies with OMB Circular A-130 policy and is consistent with the intent of NIST SP 800-34. Documented procedures shall be developed to facilitate the implementation of the contingency planning policy and associated contingency planning controls. The contingency planning policy and procedures shall be consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. Contingency planning may result in manual processes in the instance of an actual event, instead of system recovery at an alternate site.

4.2.3.2. CONTINGENCY PLAN

All major CMS systems shall be covered by a contingency plan, relative to the system security level, providing continuity of support in the event of a disruption of service. A contingency plan for the information system shall address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. A contingency plan for the information system shall be consistent with NIST SP 800-34. Designated officials within CMS shall review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

4.2.3.3. CONTINGENCY TRAINING

Operational and support personnel (including managers and users of the information system) shall receive training in contingency operations and understand their contingency roles and responsibilities with respect to the information system. Refresher training shall be provided to all contingency personnel.

4.2.3.4. CONTINGENCY PLAN TESTING

Contingency plans shall be tested periodically using defined tests and exercises to determine the plans' effectiveness and readiness to execute the plan. Test results shall be documented and reviewed by appropriate CMS officials. Reasonable and appropriate corrective actions shall be initiated to close or reduce the impact of contingency plan failures and deficiencies.

4.2.3.5. CONTINGENCY PLAN UPDATE

Contingency plans shall be periodically reviewed and, if necessary, revised to address system / organizational changes and / or any problems encountered during plan implementation, execution, or testing.

4.2.3.6. ALTERNATE STORAGE SITES

Agreements with alternate processing sites shall be established and implemented to permit the storage of CMS information system backup information. Copies of the current contingency plan shall be stored in a secure location at an alternate site accessible by management and other key personnel. Procedures shall be developed, documented, and implemented effectively to respond to contingencies by ensuring separation of routine information system operations and alternate storage sites.

4.2.3.7. ALTERNATE PROCESSING SITES

Agreements with alternate processing sites shall be established and implemented to permit the resumption of CMS information system operations for mission critical business functions when the primary processing capabilities are unavailable, and the contingency plan calls for application recovery in place of other accepted processes. Procedures shall be developed, documented, and implemented to establish contingency activities and responsibilities.

4.2.3.8. TELECOMMUNICATION SERVICES

Necessary agreements shall be established and implemented for alternate communications services capable of restoring adequate communications to accomplish mission critical functions when the primary operations and communications capabilities are unavailable.

4.2.3.9. INFORMATION SYSTEM BACKUP

Backup mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable the backing-up of user-level and system-level information (including system state information) contained in the CMS information system. The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) shall be consistent with the CMS recovery time objectives and recovery point objectives.

Mechanisms shall provide for sufficient backup storage capability. Checkpoint capabilities shall be part of any backup operation that updates files and consumes large amounts of information system time. Backup copies of CMS data shall be created on a regular basis, and appropriate safeguards shall be implemented to protect the technical and physical security of backup media. Where appropriate, backup copies of all other forms of data, including paper records, shall be created based upon an assessment of the level of data criticality and the corresponding risk of data loss.

4.2.3.10. INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Information system recovery and reconstitution mechanisms with supporting procedures shall be developed, documented and implemented effectively to allow the CMS information system to be recovered and reconstituted after a disruption or failure. Recovery of CMS information systems after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

4.2.4. CONFIGURATION MANAGEMENT (CM)

4.2.4.1. CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

A CM process that includes the approval, testing, implementation and documentation of changes shall be developed and implemented to track and control the hardware, software, and firmware components that comprise the CMS information system. The CM process shall be consistent with organization's information technology architecture plans. Formally documented CM roles, responsibilities, and procedures and documentation shall be in place.

A CM plan for the system shall be developed when the organization's plan is not adequate to address system needs. The CM plan for the information system shall be consistent with the intent of IEEE Standard 828-1998 (or successor if superseded). The CM plan shall be evaluated periodically and updated as necessary to verify the plan and the ability of those tasked to carry out the plan. Distribution of new software shall be controlled. Software licensing agreements shall be enforced and violations of those agreements shall be prohibited.

4.2.4.2. BASELINE CONFIGURATION

Procedures shall be developed, documented, and implemented effectively to maintain a baseline, operational configuration of the hardware, software, and firmware that comprise the CMS information system. An inventory of the information system's constituent components shall be maintained.

The configuration of the information system shall be consistent with the Federal Enterprise Architecture and the organization's information system architecture. The inventory of information system components shall include manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).

4.2.4.3. CONFIGURATION CHANGE CONTROL

Change control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to control changes to the information system. Change request forms shall be used to document requests with related approvals. Change requests shall be approved by the system business owner, or his / her designated representative, and other appropriate CMS officials including, but not limited to, the system maintainer and information system support staff.

Test plans shall be developed and approved for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, and library control) and shall include appropriate consideration of security. Test results shall be documented and appropriate responsive actions shall be taken based on the results.

Emergency changes for the CMS information system shall be documented and approved by appropriate organization officials, either prior to the change or after the fact. Emergency changes to the configuration shall be documented appropriately and approved, and responsible personnel shall be notified for analysis and follow-up.

4.2.4.4. MONITORING CHANGE ACTIVITY

Mechanisms to monitor change activity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to monitor information system changes and actions by privileged users. Security impact analyses shall be conducted after system changes are made to determine the IS-related effects of the changes. Activities associated with configuration changes to the information system shall be audited.

4.2.4.5. ACCESS RESTRICTION FOR CHANGE

Access control change mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enforce access restrictions associated with change control.

4.2.4.6. CONFIGURATION SETTINGS

Procedures shall be developed, documented, and implemented effectively to configure and benchmark information technology products in accordance with good security practice settings. The security settings of information technology products shall be configured to the most restrictive mode consistent with information system operational requirements.

4.2.4.7. LEAST FUNCTIONALITY

Information system shall be configured to provide only essential capabilities. The functions and services provided by CMS information systems shall be reviewed carefully to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing). The use of those functions, ports, protocols, and / or services shall be prohibited and / or restricted.

4.2.5. MAINTENANCE

4.2.5.1. SYSTEM MAINTENANCE POLICY AND PROCEDURES

System maintenance shall be employed on all CMS information systems addressing critical aspects of hardware and software maintenance including scheduling of periodic maintenance; maintenance tools; remote maintenance; maintenance personnel; and timeliness of maintenance. Maintenance of software shall include the installation of all relevant patches and fixes required to correct security flaws in existing software and to ensure the continuity of business operations.

4.2.5.2. PERIODIC MAINTENANCE

Comprehensive maintenance testing procedures shall be developed, documented, and implemented effectively to conduct periodic on-site and off-site maintenance of the CMS information systems and of the physical plant within which these information systems reside. A maintenance log for the information system shall be maintained including:

- (i). the date and time of maintenance;
- (ii). name of the individual performing the maintenance;
- (iii). name of escort, if necessary; and
- (iv). a description of the maintenance performed.

Appropriate officials shall approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, all information from associated media shall be removed using CMS approved procedures. After maintenance is performed on the information system, the security features shall be tested to ensure that they are still functioning properly.

4.2.5.3. MAINTENANCE TOOLS

The use of system maintenance tools, including diagnostic and test equipment and administration utilities, shall be approved, controlled and monitored. Approved tools shall be maintained on an on-going basis.

4.2.5.4. REMOTE MAINTENANCE

Remote maintenance of a CMS information system must be approved by the CIO or his / her designated representative. Remote maintenance procedures shall be developed, documented, and implemented effectively to provide additional controls on remotely executed maintenance and diagnostic activities.

The use of remote diagnostic tools shall be described in the system security plan for the information system. Maintenance logs for all remote maintenance, diagnostic, and service activities shall be maintained and shall be reviewed periodically by appropriate CMS officials. All sessions and remote connections shall be terminated after the remote maintenance is completed. If password-based authentication is used during remote maintenance, the passwords shall be changed following each remote maintenance service.

4.2.5.5. MAINTENANCE PERSONNEL

Maintenance personnel procedures shall be developed, documented, and implemented effectively to control maintenance of CMS information systems. A list of individuals authorized to perform maintenance on the information system shall be maintained.

4.2.5.6. TIMELY MAINTENANCE

Maintenance services and parts shall be available in a timely manner.

4.2.6. SYSTEM AND INFORMATION INTEGRITY (SI)

4.2.6.1. SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Automated mechanisms for system, software, and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to systems and software. The procedures and automated mechanisms shall be consistent with applicable federal laws, directives, policies, regulations, standards and guidance.

4.2.6.2. FLAW REMEDIATION

Information system flaws in an operational CMS information system shall be identified, reported and effective remedial actions shall be taken. Systems affected by recently announced software vulnerabilities shall be identified. Patches, service packs, and hot fixes shall be tested for effectiveness and potential side effects on the CMS information systems prior to installation. Flaw remediation process shall be centrally managed and updates shall be installed automatically without individual user intervention.

4.2.6.3. MALICIOUS CODE PROTECTION

Automated malicious code protection mechanisms that include a capability of automatic updates shall be in place and supporting procedures shall be developed, documented, and implemented effectively to identify and isolate suspected malicious software. Antiviral mechanisms shall be implemented effectively and maintained, at critical information system entry points, and at each

workstation, server, or mobile computing device on the network to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, removable media or other methods. System Owners shall use antiviral software products from multiple vendors, if possible, and update virus protection mechanisms whenever new releases are available.

4.2.6.4. INTRUSION DETECTION TOOLS AND TECHNIQUES

Effective intrusion tools and techniques providing real-time identification of unauthorized use, misuse, and abuse of the information system shall be implemented.

4.2.6.5. SECURITY ALERTS AND ADVISORIES

Procedures shall be developed, documented, and implemented effectively to establish a process for receiving IS alerts and advisories on a regular basis, and for issuing IS alerts and advisories to appropriate personnel. Upon receipt of such alerts and advisories, CMS personnel shall take appropriate response actions. The types of actions to be taken in response to security alerts / advisories shall be documented.

4.2.6.6. SECURITY FUNCTIONALITY VERIFICATION

Automated mechanisms shall be established and implemented to provide the capability for CMS information systems to verify the correct operation of security functions on a regular basis, and automatically to take appropriate response actions when security-related anomalies are discovered.

4.2.6.7. SOFTWARE AND INFORMATION INTEGRITY

Automated mechanisms for software and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to software. Good software engineering practices consistent with CMS IS policy and procedures shall be employed with regard to commercial-off-the-shelf (COTS) integrity mechanisms and automated mechanisms shall be in place to monitor the integrity of the CMS information system and applications.

4.2.6.8. SPAM AND SPYWARE PROTECTION

Automated mechanisms for spam and spyware protection shall be in place at critical information system entry points, workstations, servers, and mobile computing devices on the network. Supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect spam and spyware.

4.2.6.9. INFORMATION INPUT RESTRICTIONS

Automated mechanisms shall be in place to restrict the information input to the information system to authorized personnel. Personnel authorized to input information to the information system shall be restricted beyond the typical access controls employed by the system, including limitations based on specific operational / project responsibilities.

4.2.6.10. INFORMATION INPUT ACCURACY, COMPLETENESS, AND VALIDITY

Automated mechanisms shall verify information inputs for accuracy, completeness, and validity as close to the point of origin as possible.

4.2.6.11. ERROR HANDLING

Information systems shall identify and handle error conditions in an expeditious manner. User error messages generated by information systems shall provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages shall be revealed only to authorized personnel. Sensitive information shall not be listed in error logs or associated administrative messages.

4.2.6.12. INFORMATION OUTPUT HANDLING AND RETENTION

The organization shall handle and retain output from the information system in accordance operational requirements and the information sensitivity level.

4.2.7. MEDIA PROTECTION (MP)

4.2.7.1. MEDIA PROTECTION POLICY AND PROCEDURES

MP controls and procedures shall be developed and implemented to address media access; media labeling; media transport; media destruction; media sanitization and clearing; media storage; and disposition of media records. The MP procedures shall be consistent with applicable federal laws, directives, policies, regulations, standards and guidance.

4.2.7.2. MEDIA ACCESS

Procedures shall be developed, documented, and implemented effectively to ensure adequate supervision of personnel and review of their activities to protect against unauthorized receipt, change, or destruction of electronic and paper media based on the sensitivity of the CMS information. Automated mechanisms shall be implemented to control access to media storage areas and to audit access attempts and access granted.

4.2.7.3. MEDIA LABELING

Storage media and information system output shall have external labels affixed to indicate the distribution limitations, applicable security classification, and handling caveats of the information. Specific types of media or hardware components may be exempted from the labeling requirement, so long as the exempted items remain within a secure environment. Only the CIO or his / her designated representative shall have the authority to exempt specific types of media or hardware components from the labeling requirement.

4.2.7.4. MEDIA STORAGE

Media storage procedures shall be developed, documented, and implemented effectively to facilitate the secure storage of media, both electronic and paper. Storage media shall be controlled physically and safeguarded in the manner prescribed for the highest system security

level of the information ever recorded on it until destroyed or sanitized using CMS approved procedures.

4.2.7.5. MEDIA TRANSPORT

Physical, administrative, and technical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) to authorized personnel based on the sensitivity of the CMS information.

4.2.7.6. MEDIA SANITIZATION

Formal documented procedures shall be developed and implemented to ensure that sanitization and disposal methods are commensurate with the sensitivity and criticality of data residing on storage devices, equipment, and hard copy documents. Media sanitization actions shall be tracked, documented, and verified. Sanitization equipment and procedures shall be tested periodically to ensure proper functionality.

4.2.7.7. MEDIA DESTRUCTION AND DISPOSAL

Media destruction and disposal procedures shall be developed, documented, and implemented effectively, in an environmentally approved manner, to facilitate the destruction and disposal of media, both electronic and paper using approved methods, to ensure that CMS information does not become available to unauthorized personnel. Approved equipment removal procedures for CMS information systems and components that have processed or contained CMS information shall be followed. Inventory and disposition records for media, both electronic and paper, shall be produced, stored, updated, and retained.

4.2.8. INCIDENT RESPONSE (IR)

4.2.8.1. INCIDENT RESPONSE POLICY AND PROCEDURES

An IR plan shall be developed, disseminated and reviewed / updated periodically to address the implementation of IR controls. IR procedures shall be developed and implemented to monitor and respond to all IS incidents or suspected incidents by addressing all critical aspects of incident handling and response containment. The IR procedures shall be consistent with applicable federal laws, directives, policies, regulations, standards and guidance, including, but not limited to, NIST SP 800-61.

4.2.8.2. INCIDENT RESPONSE TRAINING

All personnel shall be trained in their IR roles and responsibilities with respect to a CMS information system. Personnel shall receive periodic refresher training in IR procedures.

4.2.8.3. INCIDENT RESPONSE TESTING

The IR capability for a CMS information system shall be tested periodically using appropriate tests, procedures, automated mechanisms and exercises to determine the plan's effectiveness. The test results, the procedures, and exercises employed to conduct the test shall be documented.

4.2.8.4. INCIDENT HANDLING

An incident handling capability, which includes preparation, identification, containment, eradication, recovery, and follow-up capabilities in response to security incidents, shall be established and maintained. Evidence of computer crimes, computer misuse, and all other unlawful computer activities shall be properly preserved. Lessons learned from on-going incident handling activities shall be incorporated into the incident response procedures.

4.2.8.5. INCIDENT MONITORING

On-going monitoring of the CMS information system for security events shall be conducted. All events and activities associated with system performance shall be monitored for the identification of resources used by processes and user activity that may indicate security threats resulting from user, software, or hardware activity. All CMS user activities shall be subject to monitoring to verify compliance with this policy and to detect actions that may be in violation of this policy.

4.2.8.6. INCIDENT REPORTING

All IS incidents, or suspected incidents, shall be reported to the CMS IT Service Desk as soon as an incident comes to the attention of a user of CMS information or information systems. Events and confirmed security incidents by business partners shall also be reported to the CMS IT Service Desk in accordance with established procedures.

4.2.8.7. INCIDENT RESPONSE ASSISTANCE

A CMS IT Service Desk shall be in place and shall play an appropriate role in the organization's IR program. The CMS IT Service Desk shall offer advice to users of a CMS information system. Procedures shall be developed, documented, and implemented effectively to facilitate incident response by providing central incident support resource for CMS information system users.

4.2.9. AWARENESS AND TRAINING (AT)

4.2.9.1. SECURITY AWARENESS & TRAINING POLICY AND PROCEDURES

An IS AT program shall be developed and implemented for all personnel, including contractors and any other users of CMS information systems. The IS AT program shall be consistent with applicable federal law, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-50. AT shall be completed by all personnel prior to granting authorization to access to CMS information systems and networks.

4.2.9.2. SECURITY AWARENESS

Procedures shall be developed, documented, and implemented effectively to ensure that CMS information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment. The IS Awareness and Training Program shall be consistent with 5 CFR Part 930 and the guidance described in NIST SP 800-50.

4.2.9.3. SECURITY TRAINING

The organization shall identify all positions and / or roles with significant information system security responsibilities. All personnel with significant information system security responsibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. Content of the security awareness training shall be determined based upon the information systems to which personnel have authorized access. The employee shall acknowledge having received the security and awareness training either in writing or electronically as part of the training course completion.

4.2.9.4. SECURITY TRAINING RECORDS

Procedures shall be developed, documented, and implemented effectively to ensure that individual IS training activities, including basic security awareness training and specific information system security training, are properly documented and monitored.

4.3. INFORMATION SECURITY TECHNICAL CONTROLS

4.3.1. IDENTIFICATION AND AUTHENTICATION (IA)

4.3.1.1. IDENTIFICATION & AUTHENTICATION POLICY AND PROCEDURES

Automated IA mechanisms shall be implemented and enforced for all CMS information systems in a manner commensurate with the risk and sensitivity of the system, network, and data. Supporting procedures shall be developed, documented, and implemented effectively to enable reliable identification of individual users of CMS information systems. The IA procedures shall be consistent with applicable federal laws, directives, policies, regulations, standards and guidance, including, but not limited to, FIPS 201, NIST SP 800-63, NIST SP 800-73, and NIST SP 800-76.

4.3.1.2. USER IDENTIFICATION AND AUTHENTICATION

Automated IA mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable unique identification and authentication of individual users (or processes acting in behalf of users) of CMS information systems. Authentication of user identities shall be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein.

4.3.1.3. DEVICE AND HOST IDENTIFICATION & AUTHENTICATION

Automated mechanisms shall be used to enable IA of the CMS information system being used and to which a connection is being made before establishing a connection.

4.3.1.4. IDENTIFIER MANAGEMENT

Procedures shall be developed, documented, and implemented effectively to manage user identifiers. The procedures shall address processes and controls for: (i) identifying each user uniquely; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate CMS official; (iv) ensuring that the user identifier is issued to the

intended party; (v) disabling user identifier after a specific period of inactivity; and (vi) archiving user identifiers. Reviews and validation of system users' accounts shall be conducted as required to ensure the continued need for access to a system. Identifier management shall not be applicable to shared information system accounts (i.e., guest and anonymous).

4.3.1.5. AUTHENTICATOR MANAGEMENT

Procedures shall be developed, documented, and implemented to manage user authenticators. The procedures shall address processes and controls for: initial authenticator content; distribution for new, lost, compromised, or damaged authenticators; revocation of authenticators; and changing default authenticators. Users shall not loan or share authenticators with other users. Lost or compromised authenticators shall be reported immediately to appropriate authority.

Selection of passwords or other authentication devices (e.g., tokens, biometrics) shall be appropriate, based on the CMS System Security Level of the information system. Automated mechanisms shall be in place for password-based authentication, to ensure that the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces automatic expiration of passwords; (iv) prohibits password reuse for a specified number of generations; and (v) enforces periodic password changes.

4.3.1.6. AUTHENTICATOR FEEDBACK

Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented to provide feedback to users during the authentication process, without compromising the authentication mechanism.

4.3.1.7. CRYPTOGRAPHIC MODULE AUTHENTICATION

Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of FIPS 140-2.

4.3.2. ACCESS CONTROL (AC)

4.3.2.1. ACCESS CONTROL POLICY AND PROCEDURES

Logical access controls and procedures shall be established and implemented to ensure that only designated individuals, under specified conditions (e.g. time of day, port of entry, type of authentication, etc.) can access the CMS information system, activate specific commands, execute specific programs and procedures, or create views or modify specific objects (programs, information, system parameter). Procedures shall be developed to guide the implementation and management of logical access controls. The logical access controls and procedures shall be consistent with applicable federal laws, directives, policies, regulations, standards, and guidance, and shall be periodically reviewed, and, if necessary, updated.

4.3.2.2. ACCOUNT MANAGEMENT

Comprehensive account management mechanisms shall be established to: identify account types (i.e., individual, group, and system); establish conditions for group membership; and assign associated authorizations. Access to the CMS information system shall be granted based on: (i) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. Proper identification and approval shall be required for requests to establish information system accounts.

Account control mechanisms shall be in place and supporting procedures shall be developed, documented and implemented effectively to authorize and monitor the use of guest / anonymous accounts; and to remove, disable, or otherwise secure unnecessary accounts. Account managers shall be notified when CMS information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers shall also be notified when users' information system usage or need-to-know changes.

4.3.2.3. ACCESS ENFORCEMENT

Access enforcement mechanism shall be developed, documented and implemented to control access between named users (or processes) and named objects (e.g., files and programs) in a CMS information system. Additional application level access enforcement mechanism shall be implemented, when necessary, to provide increased information security for CMS. When encryption of stored information is employed as an access enforcement mechanism, it shall be encrypted with FIPS 140-2 validated cryptographic modules.

4.3.2.4. INFORMATION FLOW ENFORCEMENT

Flow control shall be enforced over information between source and destination objects within CMS information systems and between interconnected systems based on the characteristics of the information.

4.3.2.5. SEPARATION OF DUTIES

The principle of separation of duties shall be enforced to eliminate conflicts of interest in the responsibilities and duties assigned to individuals. Mission functions and distinct information systems support functions shall be divided among different roles, and support functions shall be performed by different individuals, e.g., personnel responsible for administering access control functions shall not also administer audit functions. Personnel developing and testing system code shall not have access to production libraries. Access control software shall be in place to limit individual authority and information access, such that the collusion of two or more individuals is required to commit fraudulent activity. Job descriptions shall reflect accurately the assigned duties and responsibilities that support separation of duties.

4.3.2.6. LEAST PRIVILEGE

Each user or process shall be assigned the most restrictive set of privileges needed for the performance of authorized tasks.

4.3.2.7. UNSUCCESSFUL LOG-ON ATTEMPTS

Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enforce a limit of CMS-defined consecutive invalid access attempts by a user during a specified time period. Systems shall be locked after a specified number of multiple unsuccessful log-on attempts.

4.3.2.8. SYSTEM USE NOTIFICATION

An approved warning / notification message shall be displayed upon successful log-on and before gaining system access. The warning message shall notify users that the CMS information system is owned by the U.S. Government and shall describe conditions for access, acceptable use, and access limitations. The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies) and shall remain on the screen until the user takes explicit actions to log-on to the CMS information system.

4.3.2.9. PREVIOUS LOG-ON NOTIFICATION

Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to provide users with information about previous log-ons, both successful and unsuccessful.

4.3.2.10. CURRENT SESSION CONTROL

Automated mechanisms shall be in place to limit the number of concurrent user sessions, based upon the established business needs of the user, CMS and the sensitivity level of the CMS information system.

4.3.2.11. SESSION LOCK

Automated session lock mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable locking of the information system session by the user. The information system shall also detect inactivity and block further access until the user re-establishes the connection using proper identification and authentication processes.

4.3.2.12. SESSION TERMINATION

The information system shall identify and terminate inactive user sessions automatically.

4.3.2.13. SUPERVISION AND REVIEW — ACCESS CONTROL

Personnel shall be supervised and reviewed with respect to the usage of CMS information system access controls. Automated mechanisms shall be in place to facilitate the review of audit records, and any unusual activities shall be investigated in a timely manner. Changes to access authorizations shall be reviewed periodically. The activities of users with significant information system roles and responsibilities shall be reviewed more frequently.

4.3.2.14. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Based upon mission / business requirements, public access to CMS information systems without identification and authorization shall be limited to public websites and other publicly available systems. CMS information systems shall be configured to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

4.3.2.15. AUTOMATED MARKING

Automated mechanisms shall be in place to mark CMS information system output using standard naming convention, in order to identify any special dissemination, handling, or distribution instructions.

4.3.2.16. AUTOMATED LABELING

CMS information systems shall label information “in storage”, “in process”, and “in transit” with special dissemination handling or distribution instruction, in a manner consistent with this policy.

4.3.2.17. REMOTE ACCESS

Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO, or his / her designated representative. The number of users who can access the information system from remote locations shall be limited and justification / approval for such access shall be controlled, documented, and monitored. Dial-up lines, other than those with FIPS 140-2 validated cryptography, shall not be used to gain access to a CMS information system that processes organizational information unless the CIO, or his designated representative, provides specific written authorization. Periodic monitoring shall be implemented to ensure that installed equipment does not include unanticipated dial-up capabilities.

4.3.2.18. WIRELESS ACCESS RESTRICTION

Installation of wireless access points (WAP) into organizational networks shall be prohibited unless explicitly authorized, in writing, by the CIO, or his / her designated representative. Authorized WAP devices and wireless access shall be monitored on a regular basis, and wireless communications shall be secured through the use of approved encryption controls.

4.3.2.19. ACCESS CONTROL FOR PORTABLE AND MOBILE SYSTEMS

The connection of portable and mobile systems to CMS networks shall be prohibited unless explicitly authorized, in writing, by the CIO, or his / her designated representative. Prior to connecting portable and mobile systems to CMS networks, such systems shall be configured to comply with CMS IS policies and procedures. The storage and transmission of CMS sensitive information on portable and mobile information systems shall be protected with activities such as scanning the devices for malicious code, virus protection software, and disabling unnecessary hardware. The activities and controls shall be commensurate with the system security level of the information.

4.3.2.20. PERSONALLY-OWNED INFORMATION SYSTEMS

Personally-owned information systems, including, but not limited to, personal desktop computers, laptops, tablet personal computers, Personal Digital Assistant (PDA) devices, cellular telephones, and facsimile machines, shall not be used to store, access, transmit, or process CMS sensitive information, unless explicitly authorized, in writing, by the CIO, or his designated representative.

CMS shall establish strict terms and conditions for the use of personally-owned information systems. The terms and conditions shall address, at a minimum: (i) the types of applications that can be accessed from personally-owned information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally-owned information system will be prevented from accessing federal information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of virus and spyware protection software; and (viii) how often the security capabilities of installed software are to be updated.

4.3.3. AUDIT AND ACCOUNTABILITY (AU)

4.3.3.1. AUDIT & ACCOUNTABILITY POLICY AND PROCEDURES

All CMS information systems shall be configured to produce, store, and retain audit records of specific system, application, network, and user activity. Procedures shall be developed to guide the implementation and management of audit controls, and shall be consistent with applicable federal laws, directives, policies, regulations, standards and guidance, and shall be reviewed periodically, and, if necessary, updated.

4.3.3.2. AUDITABLE EVENTS

Automated mechanisms shall be established which enable the ability to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact investigations of security incidents. The selection of auditable events shall be based upon a RA as to which events require auditing on a continuous basis, and which events require auditing in response to specific situations.

4.3.3.3. CONTENT OF AUDIT RECORDS

Automated mechanisms shall be established to provide the capability to include specific information in audit records. Audit records shall contain sufficient information to establish what events occurred, when the events occurred, the source of the events, the cause of the events, and the event outcome.

4.3.3.4. AUDIT STORAGE CAPACITY

A sufficient amount of information system storage capacity shall be allocated for audit records, and information systems shall be configured to prevent audit records from exceeding such storage capacity.

4.3.3.5. AUDIT PROCESSING

Automated mechanisms shall be established which provide the capability to generate information system alerts for appropriate officials in the event of an audit failure or audit storage capacity being reached.

4.3.3.6. AUDIT MONITORING, ANALYSIS, AND REPORTING

Audit records shall be reviewed and analyzed regularly to identify and detect unauthorized, inappropriate, unusual, and / or suspicious activity. Such activity shall be investigated and reported to appropriate officials, in accordance with the CMS Incident Response Plan and CMS Incident Response Handling Procedures.

4.3.3.7. AUDIT REDUCTION AND REPORT GENERATION

Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented to enable human review of audit information and the generation of appropriate audit reports.

4.3.3.8. TIME STAMPS

Audit records shall employ time stamps for use in audit record generation. Time stamps of audit records shall be generated using internal system clocks that are synchronized system-wide.

4.3.3.9. PROTECTION OF AUDIT INFORMATION

Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

4.3.3.10. NON-REPUDIATION

Non-repudiation mechanisms shall be implemented that enable a later determination whether a given individual sent a specific message and whether a given individual received a specific message.

4.3.3.11. AUDIT RETENTION

CMS shall retain audit logs to provide support for after-the-fact investigations of security incidents, and to meet regulatory and / or organizational information retention requirements.

4.3.4. SYSTEM AND COMMUNICATIONS PROTECTION (SC)

4.3.4.1. SYSTEM & COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Technical controls shall be established and implemented to ensure the CIA of CMS information systems and the protection of the CMS information system communications. Procedures shall be developed to guide the implementation and management of such technical controls. The technical controls and procedures shall be consistent with applicable federal laws, directives,

policies, regulations, standards, and guidance, and shall be reviewed periodically, and, if necessary, updated.

4.3.4.2. APPLICATION PARTITIONING

User interface services (e.g., web services) shall be separated physically or logically from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

4.3.4.3. SECURITY FUNCTION ISOLATION

Information system security functions shall be isolated from non-security functions by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform those security functions. The system shall maintain a separate execution domain (e.g., address space) for each executing process.

4.3.4.4. INFORMATION REMNANTS

No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) shall be available to any current user (or current process) who obtains access to a shared system resource that has been released back to the information system. There shall be no residual information from the shared resource.

4.3.4.5. DENIAL OF SERVICE PROTECTION

Mechanisms shall be established to prevent, or limit the effects of well-known, detectable, and preventable Denial-of-Service attacks.

4.3.4.6. RESOURCE PRIORITY

Mechanisms shall be implemented to provide for allocation of information system resources based upon priority. Priority protection shall ensure that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.

4.3.4.7. BOUNDARY PROTECTION

Automated boundary protection mechanisms shall be established and supporting procedures shall be developed, documented, and implemented to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. Any connections to the Internet, or other external networks or information systems, shall occur through controlled interfaces. The operational failure of the boundary protection mechanisms shall not result in any unauthorized release of information outside of the information system boundary. Information system boundary protections at any designated alternate processing sites shall provide the same levels of protection as those of the primary site.

4.3.4.8. TRANSMISSION INTEGRITY

Procedures shall be developed and documented, and technical controls shall be established and implemented to protect the integrity of CMS information while in transit.

4.3.4.9. TRANSMISSION CONFIDENTIALITY

Procedures shall be developed and documented, and technical controls shall be established and implemented that protect the confidentiality of CMS sensitive information while in transit.

4.3.4.10. NETWORK DISCONNECT

Technical controls shall be established and implemented to ensure that network connections are properly terminated at the end of user sessions, or upon the occurrence of specified conditions, e.g., a period of inactivity.

4.3.4.11. TRUSTED PATH

Technical controls shall be established and implemented to provide the capability to establish trusted communications paths between authorized users and the security functionality of the information system.

4.3.4.12. CRYPTOGRAPHIC KEY MANAGEMENT

Documented procedures shall be implemented for cryptographic key generation, distribution, storage, use, and destruction. Symmetric and asymmetric keys used to protect organizational information shall be controlled and distributed using the NIST SP 800-56 and NIST SP 800-57 approved key management guidance.

4.3.4.13. USE OF VALIDATED CRYPTOGRAPHY

When encryption is used, procedures shall be developed, documented, and implemented effectively to ensure that federal requirements are met and include the use of FIPS 140-2 validated cryptography.

4.3.4.14. PUBLIC ACCESS PROTECTIONS

Technical controls shall be established and implemented to protect the integrity of the publicly accessible CMS information and applications.

4.3.4.15. COLLABORATIVE COMPUTING

Running collaborative computing mechanisms on information systems shall require authorization by the CIO, or his / her designated representative. The authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which mechanisms can be used. Collaborative computing mechanisms shall not be activated remotely.

4.3.4.16. TRANSMISSION OF SECURITY PARAMETERS

Technical controls shall be established and implemented to ensure that CMS information systems reliably associate security parameters with information exchanged between information systems.

4.3.4.17. PUBLIC KEY INFRASTRUCTURE CERTIFICATES

All public key certificates used in the information system shall be issued in accordance with a defined certification policy and certification practice statement. Registration to receive a public key certificate shall include authorization by a supervisor or a responsible official, and shall be done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

4.3.4.18. MOBILE CODE

CMS shall establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause harm to CMS information systems. CMS shall document, monitor and implement controls for the use of mobile code within the CMS information system. Appropriate officials shall authorize or deny the use of mobile code. CMS shall implement controls and procedures for mobile code in accordance with NIST SP 800-28.

4.3.4.19. VOICE OVER INTERNET PROTOCOL

CMS shall establish usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to harm CMS information systems. CMS shall document, monitor and implement controls for the use of VOIP within a CMS information system. When VOIP is implemented, CMS shall adhere to the NIST SP 800-58 guidance.

4.4. INVESTMENT MANAGEMENT LEVEL AND PROJECT MANAGEMENT LEVEL REVIEWS

This policy prompts the following Investment Management Level Reviews as part of the SDLC:

- Review of BCA SOW/393;
- Review of Business Case Analysis (BCA);
- Review of Business Risk Assessment;
- Review of SDLC SOW/393;
- Review of Data Use Agreement (DUA);
- Review of System of Records (SOR);
- Review of Computer Match Agreement (CMA);
- Review of Inter / Intra-agency Agreement (IA);
- System Certification;
- System Accreditation;
- Implementation Readiness Review (IRR); and
- System Re-Certification / System Re-Accreditation.

The reviews are defined as part of the CMS Integrated IT Investment and System Life Cycle Framework, i.e., “CMS Framework”, for software development.

5. ROLES AND RESPONSIBILITIES

The following entities have responsibilities related to the implementation of this program policy.

5.1. CMS ADMINISTRATOR

CMS Administrator has the overall responsibility for the implementation of an agency-wide IS Program as required by the laws and regulation as directed by the Department of Health and Human Services (DHHS) for ensuring compliance with all government-wide legal and policy requirements.

The CMS Administrator shall be responsible for the following duties, in accordance with provisions of FISMA:

- Provide information security protections commensurate with this policy, the CMS IS program and federal regulations.
- Ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control.
- Delegate to the CMS Chief Information Officer the authority to ensure compliance with the requirements imposed on CMS under sub-section 3544 of FISMA, Federal Agency Responsibilities.
- Ensure that CMS has trained personnel sufficient to assist CMS in complying with the requirements of this policy and related procedures, standards and guidelines.
- Ensure that the CMS Chief Information Officer, in coordination with other senior CMS officials, reports annually to the CMS Administrator on the effectiveness of the CMS IS Program, including progress of remedial actions.

5.2. CMS CHIEF INFORMATION OFFICER (CIO)

CMS CIO is responsible for the following:

- development, implementation and administration of the CMS IS Program, as well as DHHS and government-wide security directives;
- designating a Senior Agency Information Security Officer; developing and maintaining this policy, information security procedures, and control techniques to address federal requirements;
- training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and
- assisting senior agency officials concerning their responsibilities regarding information and information systems that support operations and assets under their realm of responsibility.

In addition to these responsibilities, the CIO shall ensure there is an appropriate level of protection for all CMS information resources, whether retained in-house or under the control of contractors, including the establishment of operational, management and technical safeguards. The CIO shall assist Business and System Owners in understanding their security responsibilities and shall ensure that they incorporate an acceptable level of protection for all CMS IT Systems.

5.3. DIRECTOR, SYSTEMS SECURITY GROUP (SSG)

The Director, SSG serves as principal advisor and technical authority to CMS and outside organizations on matters related to IS. The Director, SSG also serves as CMS' Senior Agency Information Security Officer with information security as the primary duties to ensure agency compliance.

The Director, SSG shall carry out the CIO's responsibilities as assigned through the CMS IS Program; possess professional qualifications, including training and experience, required to administer the functions involved in the CMS IS Program; have information security duties as his / her primary duty; and head an office with the mission and resources to assist in ensuring agency compliance with agency and federal regulations.

5.4. SENIOR ISSO

The Senior ISSO has primary responsibility to:

- Evaluate and provide information about the CMS IS Program, and communicate CMS IS Program requirements and concerns to management and personnel.
- Ensure that SSPs are developed, reviewed, implemented, and revised.
- Ensure that IS RAs are developed, reviewed, and implemented for the SSP process.
- Report information resources security incidents in accordance with the systems security incident reporting procedures developed and implemented by federal mandates, DHHS, and this policy.
- Mediate and resolve systems security issues that arise between two CMS organizations, CMS and other federal organizations, or CMS and States or contractors.
- Maintain documentation used to establish systems security level designations for all SSPs within CMS.
- Assist component ISSOs in developing local systems security for either in place SSPs or for those under active development.
- Research state-of-the-art systems security technology and disseminate information material in a timely fashion.
- Assure that ISSOs are appointed and trained.
- Develop and implement an information system security training and orientation program in accordance with the requirements from the FISMA Act of 2002.

5.5. COMPONENT ISSO

Component ISSOs have the responsibility to:

- Assist the Senior ISSO in ensuring the component adheres to federal laws, regulations, policies and CMS IS Program requirements;
- Act as the primary point of contact in the component for IS issues; and
- Participate in the technical certification of component RAs and SSPs.

5.6. BUSINESS OWNERS/PARTNERS AND SYSTEMS OWNERS/MANAGERS

Business and System Owners must assess the risk to the information and information systems over which they have responsibility. They must also ensure, through system certification, that

each CMS information system is developed, implemented, and operated according to the requirements of this policy and the *CMS IS Handbook*.

5.7. SYSTEM ADMINISTRATOR

The System Administrator shall be responsible for verifying that system security requirements of their systems are being met; establishing and communicating the security safeguards required for protecting systems based on the sensitivity levels of the information; and periodically reviewing and verifying that all users of the system are authorized and are using the required systems security safeguards, in compliance with CMS IS Program, and all related standards, guidelines, and procedures.

5.8. SYSTEM MAINTAINER / DEVELOPER

The System Maintainer / Developer shall be responsible for developing and implementing the security requirements throughout the SDLC as System Owners / Managers define the requirements of the information system. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for System Maintainers / Developers), or operational practices (e.g., awareness and training). The System Maintainer shall also be responsible for the planning and implementation for the on-going maintenance of the information system, including updates, upgrades and patches in accordance with the SDLC and this policy.

5.9. CMS EMPLOYEES

CMS employees have the responsibility to ensure the protection of CMS' information (data) and information systems by complying with the IS requirements maintained in this policy and in the *CMS IS Handbook*. Use of Agency-owned or leased equipment and resources to accomplish work-related responsibilities will always have priority over personal use. In order to avoid capacity problems and to reduce the susceptibility of Agency information technology resources to computer viruses and cyber attacks, employees shall comply with the following requirements:

- A. Personal files obtained via the Internet may not be stored on individual PC hard drives or on local area network (LAN) file servers;
- B. Official video and voice files may not be downloaded from the Internet except when they will be used to serve an approved Agency function; and
- C. Internet and e-mail etiquette, customs and courtesies shall be followed when using Agency-owned or leased equipment or resources.

5.10. USERS

Users have the responsibility to ensure the protection of CMS' information (data) and information systems by complying with the IS requirements maintained in this policy and in the *CMS IS Handbook*. CMS users shall attend required computer systems security and functional training. In addition, CMS users shall adhere to the duties, requirements and responsibilities as stated in Article 35 of the 2004 MLA.

6. APPLICABLE LAWS/GUIDANCE

The following public laws and federal guidance are applicable to this policy:

- FISMA Act of 2002;
- HIPAA, 1996;
- Medicare Modernization Act of 2003;
- The Privacy Act of 1974;
- OMB Circular A-130, Management of Federal Information Resources; and
- NIST SP 800 Series and FIPS Publications.

For additional information, refer to the CMS IS Handbook and Business Partner System Security Manual.

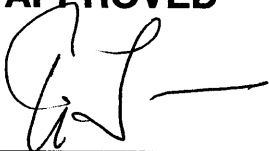
7. EFFECTIVE DATES

This policy becomes effective on the date that CMS' CIO signs it and remains in effect until officially superseded or cancelled by the CIO.

8. INFORMATION AND ASSISTANCE

Staff within the Office of Information Services, SSG are available to provide assistance in the implementation of this policy.

9. APPROVED



Timothy P. Love
CMS Chief Information Officer,

5/3/05

Date of Issuance

10. ATTACHMENTS

There are no attachments to this policy.